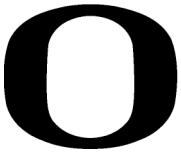

UNIVERSITY OF OREGON

APPLIED INFORMATION MANAGEMENT

Presented to the
Interdisciplinary
Studies Program:
Applied Information
Management
and the
Graduate
School of the
University of Oregon
in partial fulfillment of
the requirement for the
degree of
Master of Science

Critical Elements of an Information Security Management Strategy

CAPSTONE REPORT

Gary R. Lomprey

University of Oregon
Applied Information
Management
Program

July 2008

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved by

_____

Dr. Linda Ettinger

Critical Elements of an Information Security Management Strategy

Gary R. Lomprey

Abstract

Not only is Information Security Strategy crucial to protect information systems, but it is central to organization survival. Harris (2006) believes security strategy should be customized because each organization is unique. Literature published from 2000 to 2008 examines information systems in the context of information security. Conclusions provide discussion of six key security policy components selected from ISO-27002 (2005), spanning definitions, objectives, management goals, controls, risk assessment, policies and standards, compliance requirements, and supporting references.

Table of Contents

List of Figures and Tables

Introduction

Research Problem

Today's organizations depend on information for their survival (Whitman & Mattord, 2004, p. 2). Specifically, organizations depend on the systems and controls in place that provide for the ongoing confidentiality, integrity, and availability of their data and information (Krutz & Vines, 2004, p. 3). According to Caralli (2004) many organizations are ill-equipped to define their security goals, let alone to make an explicit connection between their security goals and the strategic drivers of the organization (p. 7). Schneier (2004) states that threats to organizational information and information systems are increasing in occurrence and in complexity and emphasizes the urgency for organizations to learn how to better protect their information and information systems (pp. 13-14).

Information security, according to the International Standards Organization (ISO), is the "protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO-27002, 2005, p. 14). Information security management, according to the National Institute of Standards and Technology's (NIST*) Information Security Handbook*, involves planning for and implementing a structure as well as the processes that provide for the alignment of information security strategy with business objectives and applicable laws and industry standards (Bowen, Hash, & Wilson, 2006, p. 11). The ISO *Information technology Security techniques: Code of practice for Information Security management* (ISO-27002, 2005) argues that information security is becoming

increasingly more important for both public and private sector businesses as the interconnection of public and private networks and the sharing of information resources increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data. Jenkins (2002) notes that information that is lost or stolen often causes financial damage and may tarnish the public image of an organization (p. 7-1). Von Solms & Von Solms (2000) believe that securing information is one of the most important aspects in any organization today and that the primary aim of information security is to protect the organization and its assets (such as sensitive information) against attempts of intrusion and corruption (p. 59).

Ross, Johnson, Katzke, Toth, Stoneburner & Rogers (2007) state that information systems are incredibly complex assemblages of technology, processes, and people that collaboratively function together to accommodate the processing, storage, and transmission of information to support an organization's mission and business functions. They argue that information security is crucial for information systems, and is central to the survival of a company. They state, "The degree to which organizations have come to depend upon [information and] these information systems to conduct routine and critical missions and business functions means that the protection [Security] of the underlying systems [and the information such systems host] is paramount to the success of the organization (Ross, et al., 2007, p. 1).

Audience and Significance

Whitman & Mattord (2004) note it is important to consider that corporate leadership expects information and the systems which transport and store information, to

be continuously accurate, secure, and functional. However, they also note that "information security is no longer the sole responsibility of [Information Technology (IT) staff] but is the responsibility of [the whole organization] all employees and managers (Whitman & Mattord, 2004, p. 2). Petty (2005), notes that Chief Information Security Officers (CISO, n.d.) are being assigned a greater level of participation in strategic business decisions due the increased need to incorporate information security strategy in overall business strategy. As such, according to Pironti (2006) the establishment of an information security strategy is cornerstone in transforming information security into a more effective proactive activity driven by organizational leadership, in contrast to the typical reactive model of information security driven by technologists (p. 1). Information security is subjective and contextual (Canal, 2005, p. 38), and according to Harris (2006), every organization's approach to a security strategy should be different and customized accordingly, because each organization has its own threats, risks, business drivers, and industry compliance requirements (n.d.).

The intended audience for this research is Chief Information Security Officers (CISO, n.d.), Information Security Managers (TIR, n.d.), Information Technology Security Program Managers (Wilson & Hash, 2003, p. 4), and IT professionals tasked with information security management responsibilities (Yourdon, 2002, p. 247). The expectation is that these professionals are responsible for information security service operations and projects, and that it is imperative for this group of professionals to have a concise, succinct, and accurate report of how they should proceed and what they should include in the development of an information security strategy (FFIEC, 2006, p. 21).

To meet this expectation, the purpose of this literature review (Hewitt, 1998, p. 5) is to provide insight into the critical elements (ISO-27002, 2005, p. viii) of an information security management strategy (FFIEC, 2006, p. 21) through reference to multiple relevant authoritative sources and perspectives within the literature. Literature is examined that explains how an organization can identify the organization-wide elements and areas that deserve the most critical attention for information security strategy to become more effective in meeting business needs (O'Bryan, 2006, p. 1) which are elements that ensure business continuity, minimize business risk, and maximize return on investments and business opportunities(ISO-27002, 2005, p. viii)**.**

Research Limitations

Timeframe

So as to provide the most "current perspective" on the topic, literature resources are chosen following the recommendations of Leedy and Ormrod (2005), who emphasize that formal literature review sources with recent copyright or publication dates should be preferred (p. 65). As such, literature with copyright or publication dates between 1998 and 2008 are chosen.

It is important to note that according to Yourdin (2002), information systems and information technology are evolving quickly and play a much more important role than they did in the 1970s to 1990s and are now part of the critical infrastructure of most organizations (p. 93). As such, because technology and the need for information security management is evolving so quickly and is more urgent since the attacks of September 11, 2001 (Yourdin, 2002), literature was chosen within the timeframe cited above. Selected

material with copyright or publication dates prior to 2000 is chosen in order to provide foundational relevance to the topic at hand.

Literature Selection Criteria

Literature sources are found and retrieved from the University of Oregon Library, EBSCO Host, ERIC, Google and Google Scholar, and material from prior University of Oregon Applied Information Management courses along with journals and publication from international, U.S. government, and professional organization dedicated to the promotion of information security standards and practices. Following the recommendation of Leedy & Ormrod (2005), only literature with stated objectives which provide relevancy and in-depth analysis related to the topic (in this case information security management) are chosen (p. 80). Authors of all literature sources are selected based on professional credentials, accredited university affiliation, and documented experience in the field of information security. The International Standards Organization (ISO) publication *Information Technology – Security Techniques Code of practice for Information Security Management* (ISO-27002, 2005) is the foundational document in this literature review. Commercial and vendor information sources such as white papers and marketing reports on information security do not meet the criteria defined above and are therefore not included in this research.

Audience and Scope Definition

This literature review is targeted at information security professionals who work in organizations charged with developing a strategy and plan for information security. While this literature review provides an annotated bibliography and report of what

multiple selected authorities currently consider to be the: (1) foundational factors and contextual background (University of North Carolina , n.d) on the topic of information security, (2) most common threats to information and information systems as well as barriers to the development of information strategy, and (3) critical elements of an information security strategy which mitigate information security threats and barriers to information security strategy development, this literature review is not intended to be an exhaustive implementation guide. Instead, information is provided to the target audience with the expectation that they can use this inquiry to better understand the critical elements of information security to be addressed and used in a comprehensive information security strategy (FFIEC, 2006, p. 21.). In this case, the notion of 'critical' refers to "ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities"(ISO-27002, 2005, p. 14)**.**

Writing Plan Preview

Obenzinger (2005), states that a literature review is a piece of discursive writing that argues some position or point of view about research and usually follows specific rhetorical patterns (p. 4). Based on his options, the rhetorical patterns selected for use in the review of literature are Swiss Cheese and Battlebot, used in combination. The Swiss Cheese approach (Obenzinger, 2005) is used to establish an overview of current knowledge in the field of information security and, from a variety of credible authors and publications, to offer several perspectives on information security and the critical elements of information security strategy. Analysis of literature from multiple sources helps identify gaps and areas of the topic which merit further investigation (p. 5). The

Battlebot (Obenzinger, 2005) rhetorical pattern is used in conjunction with the Swiss Cheese approach and identifies various lines of argument, contrast, and debate from a variety of sources in the field and then situates the current research within that context (p. 5). Another way to describe the Writing Plan is that this literature review follows a "thematic" method (University of North Carolina, n.d.), in that it is organized around a [specific] topic and the issues pertaining to the topic and is framed in a "state of the art" review format (Colorado State University, n.d.) as it concentrates mainly on the most current research in the area of information security management. The intent is that the review of literature presents perspectives from multiple authoritative sources on the topic and points out possible areas in need of further research.

Definitions

The following list of terms provides definitions derived from the selected literature as a way to reveal specific context concerning the topic of information security management. Definitions are direct citations from literature used in this inquiry.

Availability - Timely, reliable access to data and information services for authorized users (CNSS, 2003, p. 8)

Access Control - The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (Kissel, 2006, p. 4).

Business continuity - The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event or interruption (Honour, n.d.).

Chief Information Security Officer (CISO) A top level management executive in an organization who is charged with providing to the executive leadership, guidance in the subject of IT security and IT risk management. It is common for a CISO in this role to report to the Chief Information Officer (CIO) who is in charge of the information technology organization or to a Chief Technology Officer (CTO) who provides the organization with leadership in the area of technology (CISO, n.d.)

Compliance - Conforming to a specification, standard or law that has been clearly defined (ZDNET, n.d).

Confidentiality - Assurance that information is not disclosed to unauthorized individuals, processes, or devices (CNSS, 2003, p. 18).

Control - Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature NOTE Control is also used as a synonym for safeguard or countermeasure (ISO-27002, 2005, p. 19).

Critical Elements - Elements which ensure business continuity, minimizing business risk, and maximizing return on investments and business opportunities"(ISO-27002, 2005, p. viii).

Cryptography - The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. The discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity (Kissel, 2006, p. 24)

Data - Unit of information that has a unique meaning and subcategories (data items) of distinct value (Kissel, 2006, p. 25), also a binary (digital) representations of atomic facts, text, graphics, bit-mapped images, sound, analog or digital live-video segments. Data is the raw material of a system supplied by data producers and is used by information consumers to create information (E-Literal, n.d.).

Data Integrity - The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit (Kissel, 2006, p. 25).

Due Diligence - The Process of taking every reasonable precaution in the circumstances for the protection of the asset under review or in question (Peltier, 2005, p. 325).

HIPAA - Acronym that stands for the Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers (HIPAA, n.d)

Information - Data that has been processed to add or create meaning and hopefully knowledge for the person who receives it. Information is the output of information systems (E-Literal, n.d.).

Information Security – The protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO-27002, 2005, p. 14).

Information Security Management – Planning for and implementing a structure as well as the processes that provide for the alignment of information security strategy with business objectives and applicable laws and industry standards (Bowen, Hash, & Wilson, 2006, p. 11).

Information Security Strategy - A plan to mitigate information security risks while complying with legal, statutory, contractual, and internally developed requirements. Typical steps to building a strategy include the definition of control objectives, the identification and assessment of approaches to meet the objectives, the selection of controls, the establishment of benchmarks and metrics, and the preparation of implementation and testing plans (FFIEC, 2006, p. 21.).

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Kissel, 2006, p. 40).

Information Technology – The different techniques required to perform the task of information systems processing. These technology units within the information systems organization are required to be orchestrated by the information systems head (Jenkins, 1999, pp. 9-12).

I**ntegrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity (Kissel, 2006, p. 40).

International Standards Organization (ISO) - The world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system (International Standards Organization, n.d).

Metrics – Measures used to indicate levels of achievement or progress. (Sundaram, May 2008, p. 24)

Policy – A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance (Kissel, 2006, p. 56)

Risk – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring (Kissel, 2006, p. 40).

Risk Management – The process of identifying, assessing, and reducing the risk to an acceptable level and implementing the right mechanisms to maintain that level of risk (Harris, 2003, p. 882).

Safeguards – Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures (Kissel, 2006, p. 67).

Threat - Any circumstance or event with the potential to adversely impact information and information systems through unauthorized access, destruction, disclosure, modification of data, and/or denial of service (CNSS, 2003, p. 61).

Vulnerability – A weakness of an asset or group of assets that can be exploited by one or more threats (ISO-27002, 2005, p. 3).

Research Parameters

The research parameters section provides insight into the methods and framework used in the development of this inquiry and includes the following sub-sections: search report, literature evaluation selection criteria, and a writing plan. The search report section includes a list of search engines and databases used in the literature search as well as the actual search terms used to find literature pertinent to the topic. The literature evaluation selection criteria section includes subsections describing how relevance and audience are defined and how authors and publishers are chosen. The writing plan section is a roadmap which frames how information and concepts are to be collected and presented in the Review of the Literature.

Search Report

This search report is a review and summary of the resources and methods used in locating literature relevant to the field of information security strategy (FFIEC, 2006, p. 21), information security (ISO-27002, 2005, p. 14) and information security management (Bowen, Hash, & Wilson, 2006, p. 11). The criteria used to determine the quality of the search request results are based on the level of relevancy to information security strategy (FFIEC, 2006, 21), information security (ISO-27002, 2005, p. 14), information security management (Bowen, Hash, & Wilson, 2006, p. 11), audience, and number of results returned. Relevancy is depicted in four levels: Poor, Fair, Good, and Excellent.

Search Engines and Databases

. Searches were performed on the following search engines and databases:

- Carnegie Mellon Institute – Computer Emergency Response Team (CERT) database
- EBSCO HOST Research Databases – Academic Search Premier
- Google
- Google Scholar
- National Institute of Standards and Technology (NIST) database
- National Security Agency (NSA) database
- SANS Institute database
- University of Oregon Libraries Catalog

Topic Area Search Terms

Information Security

Information Strategy & Definition

Information Security & Strategy & Definition

National Institute of Standards and Technology & Glossary

Information Security Teams

Chief Security Officer & Information security management

The search engine and database search results are displayed in the Summary Table of Search Results (see Figure 1).

Search Engine / Database	Search Terms	Results	Quality of Results

Google	Information Strategy & Definition	28,100,00	Good
	Information Security & Strategy & Definition	728,000	Good
	National Institute of Standards and Technology & Glossary	1,390,000	Fair
	Information Security Teams	13,300,000	Poor
	Chief Security Officer & Information security management	3,060,000	Fair
SANS Institute database	Information Strategy	13	Good
	Information Security & Resiliency	23	Excellent
	Information Security Teams	13	Fair
National Institute of Standards and Technology (NIST) database	Information Strategy & Definition	4	Good
	Information Security & Strategy & Definition	4	Good
	Information Security Teams	5	Fair
Carnegie Mellon Institute – Computer Emergency Response Team (CERT) database	Information Strategy & Information Resiliency	53	Good
	Information Security & Strategy & Definition	5	Good
	Information Security Teams	18	Fair
National Security Agency (NSA) database	Information Strategy & Definition	5	Good

	Information Security & Strategy & Definition	11	Fair
	Information Management & Business Continuity	34	Fair
U of O Library, ECO and Summit Catalog (Using the Multiple database search function)	Information security and Importance	160	Poor
	Importance of Information security	160	Poor
	Information security issues	584	Fair
	Information resilience	210	Fair
	Information security explained	18	Fair
	Information security strategy	211	Poor
Google Scholar	Information security and importance	1,840,000	Good
	Importance of information security	1,820,000	Good
	Information security issues	2,120,000	Good
	Information resilience	135,000	Fair
	Information security explained	1,000,000	Good
	Information security strategy	1,440,000	Excellent
Google	Information security and importance	4,960,000	Good
	Importance of information security	4,400,000	Fair
	Information security issues	1,300,000	Fair
	Information resilience	902	Good
	Information security explained	1,280,000	Fair
	Information security strategy	14,000,000	Good
EBSCO Host	Information security and importance	0	Poor
	Importance of information security	12	Good
	Information security issues	20	Fair
	Information resilience	503	Poor

	Information security AND explained	7	Fair
	Information security strategy	11	Good

Figure 1: Summary Table of Search Results

Literature Evaluation and Selection Criteria

Following the method outlined by Leedy & Omrod (2005), literature is initially compiled and tested for quality by scanning indexes and abstracts of publications such as books, articles and research papers in the area of information management (p. 66). A reference librarian at the University of Oregon library also provided insights into where to find literature relevant to the topic of information management.

Relevance.

Literature is chosen based on the premise that it addresses the original research question (Bell & Smith, 2008). Primary sources of literature provide the foundational material which supports the research question and secondary sources of literature provide supporting and cross-references perspectives (Ormondroyd, Engle, & Cosgrave., 2004).

Author.

Authors of the literature used in this literature review are chosen following the Cornell University Library guidelines (Ormondroyd, Engle, & Cosgrave., 2004) for appraising authors:

- The author's credentials—institutional affiliation or where the author has worked or performed research, Educational Background, past writings, and if the author's publications are written in the author's principal area of expertise.
- How often the authors cited by other publications or quoted by other authors in the field of information security management. Quoting circles are checked by how often an author's works are cited by other authors and publications from different publishers.

- The author's dedication to the subject matter, as noted by years of experience and contribution to the promotion of information security management.
- How the author states the goal of the material and how well the author presents and argues her or his position.

Publisher.

Publishers are considered in the same fashion as authors and are chosen based on their reputation for publishing scholarly and expert level material (Ormondroyd, Engle, & Cosgrave., 2004). Publishers included in this literature review are accredited national and international Universities, United States Government agencies, reputable national and international standards organization, and reputable publishers of the works of respected authors in the information security management industry (Bell & Smith, 2008). Popular magazines, as well as vendor and industry white papers are considered anecdotal and are excluded from this research due to possible commercial bias. However, in some cases publishers of industry periodicals are chosen when the author of the material found in these types of publications followed the criteria depicted in the "*Author*" section above and are considered reputable, scholarly, and expert level (Bell & Smith, 2008).

Audience.

With regards to the intended audience, only literature which addresses the concerns and research questions of scholarly and professional audiences in the information security management arena (Ormondroyd, Engle, & Cosgrave., 2004) is chosen. Focus is on information deemed to be critical to an information security strategy that is effective in "ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities"(ISO-27002, 2005, p. 14).

Writing Plan

The writing plan supports the purpose of this literature review (Hewitt, 1998, p. 5) which is to provide insight into the critical elements (ISO-27002, 2005, p. viii) of information security management strategy (FFIEC, 2006, p. 22), (these elements are more clearly identified and defined in the Review of Literature section), through reference to multiple relevant authoritative sources and perspectives within the researched literature. Two rhetorical patterns, Swiss Cheese and Battlebot, defined by Obenzinger (2005) are chosen as a way to structure the ideas collected and presented in the Review of the Literature Following the Swiss Cheese rhetorical pattern, the Review of the Literature section provides a picture of current knowledge in the field of information security and, from a variety of credible authors and publications, offers several perspectives on information security and the critical elements of information security strategy. Following Obenzinger's (2005) definition of the Battlebot rhetorical pattern, this study also identifies various lines of argument, contrast, and debate from multiple perspectives in the field, and provides a report of the findings of the research. The writing plan organizes the review of the literature into three distinct sections along with a conclusion, designed for the needs of the intended audience for this inquiry.

Writing Outline

Part one. In Part one, following the Swiss Cheese rhetorical pattern, multiple authoritative sources provide foundational knowledge and a contextual background on the information security management field and industry. An overview is provided of the

concepts and components of information security (Whitman & Mattord, 2004). The idea that information security is not a new concept (Allen, 2002) is explored, revealing that the need to protect information has existed for millennia. This section also addresses how the rapid evolution of interconnected information systems (Harris, 2003) via data communication channels has created greater opportunities as well as greater risks to privacy and the protection of organizational information assets. Historical events such as the attacks of September 11, 2001, as described by Yourdin (2002) and Information Warfare in the form of ongoing attacks on government and private sector information systems (Warren & Hutchinson, 2000) are presented in order to provide evidence for the increasing need for an organization to have an effective information security strategy (FFIEC, 2006, p. 21).

Part two. According to Harris (2003) threats to an organization's information security come in a variety of fashions and have external and internal sources (p. 49). Part two of the Review of Literature summarizes the most common threats and vulnerabilities to organizational information and information systems as well as explores their potential impact on organizational and business continuity (Krutz & Vines, 2001). This part also identifies barriers (Caralli et al., 2007) that impede the evolution of information security within organization.

Part three. Using supporting arguments derived from the selected literature, part three of the Review of Literature identifies and presents the critical elements, as defined by the International Standards Organization (ISO-27002, 2005), of an information

security strategy which mitigate information security threats and barriers identified in Part two of the writing plan. The critical elements identified by the International Standards Organizations (ISO-27002, 2005), following Obenzinger's (2005) Battlebot rhetorical pattern, are also presented via multiple perspectives and interpretations from a variety of authors, publishers, and authorities. In some cases, these elements are identified as domains of information security such as described by the International Information Systems Security Certification Consortium ((ISC)², n.d).

Conclusion. As suggested by the Battlebot rhetorical pattern (Obenzinger, 2005), the conclusion of the Review of Literature provides additional perspectives re-framed for the needs of the intended audience through text, tables (Sevilla, 2002, p. 145) and illustrations from selected sources.

Annotated Bibliography

This Annotated Bibliography is a list of 20 core references used to write the Review of the Literature section. The references in this bibliography provide a selected compilation of current, reputable, and authoritative publications in the area of information security management, according to the literature collection and selection criteria noted above. Annotation consists of a bibliographic citation and abstract for each publication, as well as an explanation of assessment of credibility and a statement as to how the work was used to support this inquiry.

Bowen, P., Hash, J., & Wilson, M. (2006) Information Security Handbook: *A Guide for Managers. National Institute of Standards and Technology publication 800-100*. Retrieved April 14, 2008 from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

ABSTRACT: Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. The topics within this document were selected based on the laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996, the Federal

Information Security Management Act (FISMA) of 2002, and Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making process for developing an information security program. National Institute of Standards and Technology (NISTIR) Interagency Report 7298 provides a summary glossary for the basic security terms used throughout this document. This handbook is cited in different sections of this inquiry to help define the role of information strategy in an organization and presents the key aspects to implementing an information security strategy. The sponsoring publisher, The National Institute of Standards and Technology (NIST) is a leading authority of standards for technology in United States. The authors are regular contributors to NIST and their works are used in several industry guidelines.

Caralli, R. (2004) The Critical Success Factor Method: *Establishing a Foundation for Enterprise Security Management*. *Carnegie-Mellon Engineering Institute Journal Article*. Retrieved April 9, 2008 from http://www.cert.org/archive/pdf/04tr010.pdf

ASTRACT: Every organization has a mission that describes why it exists (its purpose) and where it intends to go (its direction). The mission reflects the organization's unique values and vision. Achieving the mission takes the participation and skill of the entire organization. The goals and objectives of every staff member must be aimed toward the mission. However, achieving goals and objectives is not enough. The organization must perform well in key areas on

a consistent basis to achieve the mission. These key areas unique to the organization and the industry in which it competes can be defined as the organizations critical success factors. The critical success factor method is a means for identifying these important elements of success. It was originally developed to align information technology planning with the strategic direction of an organization. However, in research and fieldwork undertaken by members of the Survivable Enterprise Management (SEM) team at the Software Engineering Institute, it has shown promise in helping organizations guide, direct, and prioritize their activities for developing security strategies and managing security across their enterprises. This report describes the critical success factor method and presents the SEM team's theories and experience in applying it to enterprise security management. Richard Caralli is a professor at Carnegie Mellon University and frequent lecturer on the topic of Information security. He is also a regular contributor to the Carnegie Mellon Software Engineering Institute library of information security publications and his works are frequently cited in information security journals. This publication authored by Caralli provides an in-depth view of aligning organizational business with information security strategy. Sections of Caralli's text are used in this inquiry to provide insight into the difficulties of aligning information security strategy with business strategy. Caralli emphasizes that proper alignment of information security with business strategy is part of an essential component of an information security strategy.

Caralli,R., Stevens, C., Wallen, D., White, W., Wilson,W., & Young, L. (2007)

Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes. Technical Report CMU/SEI-2007-TR-009 ESC-TR-2007-009 Carnegie - Mellon University. Retrieved May 5, 2008 from www.cert.org/archive/pdf/07tr009.pdf

ABSTRACT: The text emphasizes the growing role of information security and business continuity in organization in the public and private sectors. The text provides support the business continuity element of an information security strategy. The author ties the paradigm of information security strategy into a bigger organizational paradigm of organizational sustainability and resiliency. The authors of the publication are university professors, information security professionals, and business leaders. The Carnegie Mellon University Computer Emergency Response Team (CERT®) is sponsored in part by grants from the U.S. government. Ideas from this publication are used to define the notion of risk management which is considered a critical element of Information security.

FFIEC (2006) *IT Handbook InfoBase*. Retrieved April 17, 2008 from http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

ABSTRACT: The "FFIEC InfoBase" was developed by the Task Force on Examiner Education to provide field examiners in financial institution regulatory agencies with a quick source of introductory training and basic information. The long-term goal of the InfoBase is to provide just-in-time training for new regulations and for other topics of specific concern, such as information security,

to examiners in FFIEC's five member agencies the: Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision. The text is important to this inquiry as it sets the definition of what an information security strategy is and provides insights into the components of an information security strategy. The Federal Reserve Board of the United States is one of the main sponsors of this document.

Harris, S. (2003) *Certified Information Systems Security Professional (CISSP) All-In-One Exam Guide 2nd ed*. Emeryville, CA: McGraw-Hill / Osborne.

ABSTRACT: Shon Harris is a CISSP, MCSE and President of Logical Security, a firm specializing in security educational and training tools. Shon is a former engineer in the Air Force's Information Warfare unit, a security consultant and an author. She has authored two best selling CISSP books, including *CISSP All-in-One Exam Guide*, and was a contributing author to the book *Hacker's Challenge*. Shon is also the co-author of *Gray Hat Hacking: The Ethical Hacker's Handbook*. The *Certified Information Systems Security Professional (CISSP) All-In-One Exam Guide* is an exhaustive guide to information systems security. Although the text touts the name “Exam Guide” it is more than a guide to passing the Internet Security Consortium’s (ISC)² CISSP Exam. The text also serves a complete reference guide for developing an information security strategy in small to very large organizations. This text provides many citations for this inquiry, as it

provides foundational knowledge of information security and offers insights and different explanations of many of the critical elements of information security.

Honour, D. (Ed.) (n.d.) *Defining Business Continuity*. Web Article. Retrieved April 17, 2008 from http://www.continuitycentral.com/feature0398.htm

ABSTRACT: This is an article explaining the definitions of basic elements of Business Continuity as they relate to information security management. The author, David Honour, is the editor of Continuity Central, a professional website dedicated to Business Continuity and Risk management. This web article takes the notion of business continuity, which is a critical element of information security strategy, and explains its two most important components: Business Continuity Planning and Business Continuity Management. The author's unique explanation of Business Continuity is used in this inquiry to provide additional perspective on the topic.

ISO-27002 (2005) Information technology Security techniques: *Code of practice for Information Security management. International Standards Organization (ISO) document*. Reference number ISO/IEC 27002:2005(E).

ABSTRACT: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual

interest. ISO/IEC 27002 (also known as ISO/IEC 17799:2005) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objective of this Standard is to provide general guidance on the commonly accepted goals of information security management. The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities. The ISO/IEC 27002:2005 is the definitive guide to the practice of information security in public and private sector organizations and serves as a base for industry security standards such as Sarbanes Oxley and HIPAA. This publication is cited heavily throughout this inquiry and is used as a base for defining the critical elements of information security and how they fit in an information security strategy.

Jenkins, G. (1999) Information Systems: *Policies and Procedures Manual 1999 Supplement.* Paramus, NJ: Prentice Hall

ABSTRACT: The Information Systems: Policies and Procedures Manual 1999 Supplement is a guide, model, and frequent decision-making reference for organizational information systems and information security policy development. The text defines common threads that link all information systems operations, providing for a variety of situations. The author, Dr. George Jenkins, is currently

a Professor of Systems Analysis with the University of Findlay and has 30 years developing policy and procedure manuals in corporations such as General Electric. Dr. Jenkins has authored articles in the *Journal of Systems Management* and the *Data Management* magazine and is also the author of *Data Processing Policies and Procedure Manual.* This text is used in this inquiry to provide insight into the development of an information security policy. It also provides a definition of Information Security Policy and examples of how Information Security Policy mitigates information security threats and vulnerabilities.

Kissel, R. (Ed.) (2006) National Institute of Standards and Technology: *Glossary of Key Information Security Terms*. [E-Version] Retrieved April 1 5, 2008 from http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

ABSTRACT: This is a glossary of security terms has been extracted from National Institute of Standards and Technology. NIST Federal Information Processing Standards (FIPS) and the Special Publication (SP) 800 series. The terms included are not all inclusive of terms found in these publications, but are a subset of basic terms that are most frequently used. The purpose of this glossary is to provide a central resource of definitions most commonly used in NIST security publications as well as academic and professional journal dedicated to information security management. NIST is a U.S government sponsored organization and its publication are considered definitive guidelines of standards

for information security. This document is important to this inquiry as it provides the most authoritative definitions of information security terms which are cited throughout this inquiry.

Krutz, R. & Vines, R. (2001) CISSP Prep Guide: *Mastering the Ten Domains of Information Security*. New York, N.Y.: Wiley & Sons.

ABSTRACT: This publication examines the information needed to pass the Internet Security Consortium's ((ISC)²) Certified Information Security Professional (CISSP) certification. As such, this book also serves an excellent desk reference for information security professionals. Dr. Ronald Krutz is a Ph.D in computer science and was key contributor in the development HIPAA (HIPAA, n.d). Dr. Krutz conducts and sponsors applied research and development in the areas of information security. Russell Vines is President and founder of the RDV Group, Inc, and is an information security consultant to the U.S. government. He is an instructor for the Internet Security Consortium's ((ISC)²) Certified Information Security Professional (CISSP) certification and is a frequent speaker on information security issues. This book provides foundational insight into the history of information security as well as perspectives on information security threats.

O'Byran, S. (2006) Critical Elements of Information Security Program Success. Volume 3, Journal Article. Retrieved April 8, 2008 from http://ww.isaca.org/Template.cfm?Section=Home&CONTENTID=34808

&TEMPLATE=/ContentManagement/ContentDisplay.cfm

ABSTRACT: The author, Sharon O'Bryan, is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Auditor (CISA) and is considered a pioneer in information security, business and technology continuity planning, and IT audit. She is also a contributor in various areas of technology law. She has been an active participant in executive strategy and risk management oversight, and corporate policy and governance committees. She has held positions as chief information security officer and chief privacy officer. She is currently an adjunct faculty member at ITT Chicago-Kent School of Law and ITT Stuart Graduate School of Business. This journal article from the Information Systems Audit and Control Association (ISACA) web site provides this inquiry contrasting perspectives on the critical elements of an information security strategy. The text is also cited in this inquiry to emphasize the importance of obtaining support from upper management and other organizational departments when developing and information security strategy.

Pettey, C.(2005*) Gartner Highlights the Evolving Role of CISO in the New Security Order* Online Article Retrieved May 16, 2008 from http://www.gartner.com/press_releases/asset_135714_11.html

ABSTRACT: This article articulates the growing role of the Chief Information Security Officer (CISO) in organizations today and succinctly makes a case how the proper alignment of business strategy with information security technologies, policies, and strategies under the direction of a qualified CISO is instrumental in

moving an organization to the next security stage and ultimately towards operations excellence. The author, Christie Petty, is regular contributor of articles dedicated to Information Security for Gartner Inc. Gartner, Inc. is the leading provider of research and analysis on the global information technology industry. Gartner serves more than 10,000 clients, including chief information officers and other senior IT executives in corporations and government agencies, as well as technology companies and the investment community. Gartner's businesses consist of Research and Events for IT professionals; Founded in 1979, Gartner is headquartered in Stamford, Connecticut, and has over 3,900 associates, including more than 1,100 research analysts and consultants, in more than 75 locations worldwide. This inquiry cites the sections of this article that provide insight into the evolving role of information security in organization as well as the growing responsibilities of the Chief Information Security Officer.

Pironti, J. (2005) *Key Elements of an Information Security Program*. Information Systems Control Journal, Vol. 1. Retrieved April 14, 2008 from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23540

ABSTRACT: This article defines the most essential elements of an information security program. John Pironti is an enterprise solutions architect and security consultant at Unisys. In this position, he has designed and implemented enterprise-wide electronic business solutions, information security programs, and threat and vulnerability management solutions for key customers including

American Express, Boeing, Citizens Bank, Embraer Aircraft Corporation, Microsoft, Kemper Investments, Sun Microsystems and Starwood Hotels. Pironti is a published writer and a frequent speaker on electronic business topics at domestic and international industry conferences. This inquiry cites sections of this article which emphasize the importance of information security in an organization and offer perspective on what should be incorporated into an information security strategy.

Ross, R. Johnson, A., Katzke, S., Toth, P., Stoneburner, G., Rogers, G, (2007) *Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans. NIST Special Publication 800-53A*. Retrieved April 14, 2007 from http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf ABSTRACT: The purpose of this publication is to provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in NIST Special Publication 800-53 (as amended), Recommended Security Controls for Federal Information Systems, and any additional security controls developed by the organization. The text provides this inquiry with citation that explanation of the nature of information systems as well as reference to the proper assessment of information security controls and

how these controls can be applied to mitigate threats to information and information systems.

Schneier, B. (2004) Secrets & Lies: *Digital Security in a Networked World*. Indianapolis, Ind.: Wiley Publishing Inc.

ABSTRACT: The author Bruce Schneier, is the founder and CTO of Counterpane Internet Security, Inc. a recognized leader in network security services. He has also authored the bestselling book *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* and *Applied Cryptography*. Schneier provides an excellent overview of the different categories of information threats, from viruses to corporate espionage and provides the steps to be taken to make information and information systems more secure.

Von Solms, E. & Von Solms, S.H. (2000) *Information Security Management Through Measurement*. In S. Qing & J.H.P. Eloff (Eds*.) Information Security for Global Information Infrastructures* (pp. 59 – 68). Norwell, MA: Kurwell Academic

ABSTRACT: The paper suggest a model, based on the continuous measuring and monitoring of information security parameters, by which information security management can be made more dynamic and relevant. The authors are part of an information security research team from the University of South Africa. Sections of this scholarly paper are cited in this inquiry to emphasize how information security should be measured and monitored.

Warren. M. & Hutchinson, W (2000) *Information Warfare: Fact or Fiction* In S. Qing & J.H.P. Eloff (Eds.) *Information Security for Global Information Infrastructures* (pp. 411 - 420). Norwell, MA: Kurwell Academic.

ABSTRACT: The paper is a result of graduate research performed by the authors at Deakin University in Victoria Australia. The aim of this paper is to explore what Information Warfare is and the impact that it could have upon a country. The paper also describes the steps that some countries, such as Australia and the U.K, are taking to protect themselves against the threat of Information Warfare. This inquiry cites sections of this paper that provide an insight of the serious nature of protecting information systems and potentially grave consequences of not properly securing information systems.

Whitman, M., & Mattord., (2004) *Management of Information Security*. Boston, Ma: Thomson.

ABSTRACT: Michael Whitman is a Ph.D and associate professor of Information Systems in the Computer Science Department at Kennesaw State University. Herbert Mattord M.BA has over 24 years in the information technology industry as an application developer and manager. Mr. Mattord is also an instructor of Information Systems in the Computer Science Department at Kennesaw State University. Both authors have extensive professional and academic careers. This textbook is used in information security management classes in graduate programs at the University Oregon and Norwich University The book provides a guideline for implanting information security in an organization. This inquiry

cites several sections of the book in order to provide historical knowledge, explain concepts, provide examples, and support other publication used in this inquiry.

Wilson. M & Hash, J. (2003) *Building an Information Technology Security Awareness and Training Program*. National Institute of Standards Technology (NIST) Special Publication 800-50. Retrieved May 5, 2008 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

ABSTRACT: This document provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's IT security program. The guidance is presented in a life-cycle approach, ranging from designing (Section 3), developing (Section 4), and implementing (Section 5) an awareness and training program, through post-implementation evaluation of the program (Section 6). Sections of this document that include guidance on how IT security professionals can identify awareness and training needs, develop a training plan, and get organizational buy-in for the funding of awareness and training program efforts are cited in this inquiry.

Yourdin, E. (2002) Byte Wars: *The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall

ABSTRACT: Text dedicated to the discussion of the impact of the terrorists attacks of September 11th 2001 and how said attacks have affected the security of information in the U.S. government and U.S. corporations worldwide. The author, Ed Yourdin, is a computer consultant, author and lecturer and holds Bachelors of Science in mathematics from the Massachusetts Institute of

Technology (MIT). The book offers convincing evidence of why information security management is essential for organization and explains what the roles management, employees, customers, and citizens play in the protection of information. This inquiry cites Yourdin's accounts of historical information security breaches and tragedies as well as his compelling suggestions to mitigate catastrophic data loss in public as well as private sector organizations.

Review of the Literature

The purpose of this literature review is to provide insight into the critical elements (ISO-27002, 2005, p. viii) of an information security management strategy (FFIEC, 2006, p. 21) through reference to multiple relevant authoritative sources and perspectives within the literature. Literature is examined that explains how an organization can identify the organization-wide elements and areas that deserve the most critical attention for information security strategy to become more effective in meeting business needs (O'Bryan, 2006, p. 1) which are elements that ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO-27002, 2005, p. viii)**.** The review is organized into three distinct sections, designed for the needs of the intended audience for this inquiry.

Part One: Contextualizing the Examination of Information Security

Part one provides contextual examination of information security through exploring historical references of protecting information, providing background knowledge of the evolution of information technology and revealing the importance of information security due to the world's growing reliance on information systems

Historical examples. According to Krutz & Vines (2001), the notion of protecting information assets is not a new one as nations, governments, and commercial organizations throughout history have sought to protect their information assets (p. 134). To illustrate this point, they state that as far back as 3000 BC, Egyptians employed a form of cryptography (Kissel, 2006, p. 24) called hieroglyphics to conceal and protect writings

from unintended recipients. Around 50 B.C. Julius Caesar, the emperor of Rome ordered that messages be sent to commanders in the field using a form of cryptography called a cipher substitution which basically shifted the letter of the alphabet by three. According to Lucas (1995), in order to protect information from being intercepted and understood by unintended recipients or enemies, Thomas Jefferson, while serving as George Washington's secretary of state from 1790 to 1793, developed a cryptographic system involving an apparatus using a stack of 26 wooden wheels and the letters of the alphabet were inscribed on the edge of each wheel. By turning the wheels, words could be scrambled and unscrambled (n.d.). She also states that this form of cryptography developed by Jefferson went through several iterations of improvements and was used effectively in the Civil War and World War I. Krutz & Vines (2001) state that during World War II Japanese and German armies used their own methods of protecting information during its storage and transmission over communication channels and that one of the major contributors to victory by the Allied Forces was the United State's military intelligence ability to intercept and decipher Japanese and German secret information (p. 138).

Information systems evolution. According to Harris (2003), computing systems from the 1960s to the 1980s experienced exponential improvement in speed and data storage capacity and the price of such information systems also became more accessible for smaller organizations. However, Harris further notes that until the 1980s the only computers available were mainframe computers which were, for the most part, self-contained with no interconnection with extraneous computing systems (p. 17). She also

states that during this time frame mainframe computers did not typically connect to other mainframe computers and that when there was a need for interconnection, it was done in a "crude fashion" for specific tasks (Harris, 2003, p. 18). At this point in time organizations did not fully depend on these systems for their survival and information security was merely an issue of securing the physical computer and its media, making sure the equipment was not stolen, damaged, or modified (Lewis University, n.d.). As information technology such as computer hardware equipment and software applications evolved, corporations increased their demand to harness the power and benefits of these technologies and thus become more dependent on them, notably so when personal computers, or PCs, were introduced in the 1980s (Allen, 2002, p. 1).

In the 1980s and 1990s the evolution and popularity of personal computers (PCs) in homes, businesses, and government agencies allowed for autonomous computing so that computers did not solely depend on one mainframe computer, but were now able to connect to multiple computers simultaneously via distributed, client-server computing architectures also known as networks (Allen, 2002, p. 1). Allen (2002), states that almost all organizations moved to the client-server or network model as it provided organizations the ability to sustain a visible business presence with other organizations, customers, partners, and suppliers (p. 1). Harris (2003) emphasizes that the popularity of PCs and networking for a larger audience caused computer technology to evolve rapidly in order to accommodate user demands for a variety of interfaces and applications; security and stability were not emphasized in the development of such the applications and operating systems (Harris, 2003, p. 18). Ultimately, what has emerged is the phenomenon known as the Internet, a labyrinth of computer networks boasting various

degrees of security (or insecurity) attempting to access and share data [information] openly as well as clandestinely (Lewis University, n.d.).

The evolution of information systems and information technology, according to Scheier (2003), will continue and will follow Moore's law which predicts that the industry will double computing power of a microchip every 18 months and that the next generation of computing devices will be smaller faster, more available, and less expensive than ever before (p. 31).

Increased importance of information security. Whitman & Mattord (2004) state that in today's global markets, organizations of all types are dependent on and enabled by information technology, which is the instrument that receives, stores, and transports information (p. 2). Harris (2003) emphasizes that public utilities, military defense systems, financial institutions, medical facilities, and every possible business sector are dependent on information technology. As a result, he points out that the level of dependence and the extent of integration that technology has attained in our lives makes information security a much more necessary and essential discipline to be addressed (p. 20).

Ross et al. (2007) state the degree to which organizations have come to depend upon information and information systems to conduct routine and critical missions and business functions means that the protection of the underlying systems [and the information such systems host] is paramount to the success of the organization (p. 1). The International Standards Organization (ISO) document ISO-27002 (2005) also emphasizes that information and the supporting processes, systems, and networks are

important business assets and further emphasizes the importance of protecting an organization's information stating that "defining, achieving, maintaining, and improving information security may be essential to maintaining a competitive edge, cash flow, profitability, legal compliance, and commercial image" (p. viii).

Yourdin (2002) in his book *Byte Wars* indicates that the devastating affects of the attacks of September 11, 2001 on New York City and the Pentagon stresses the need for organizations to have a paradigm shift regarding how they address the protection of their information and information systems. Yourdin (2002) states that valuable information is volatile and vulnerable; once it is destroyed it may possibly never be restored if not properly protected (p. 80).

ISO-27002 (2005) states that organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated (p. viii).

Information systems and computer technology are also used to steal money, gain personal financial information, and steal individual identity. Some government agencies and organizations use what is called Information Warfare (Harris, 2003) to gather tactical information, intercept competitor's secrets, and in some cases cause destruction of the competitor's information (p. 21). Warren and Hutchinson (2001) state that Information Warfare is concerned with damaging a country's National Information Infrastructure (NII) which they define as the physical and virtual backbone of an information society and includes at a minimum:

- Government networks (i.e., Executive and agency offices)
- Banking and financial network including stock exchanges, money transfers
- Public utility networks and Telecommunications
- Emergency services network (including medical, police, fire, and rescue)
- Private corporate and institutional networks
- Educational and research networks.

(p. 412).

Scheier (2003) also points to the existence of the 'infowarrior', defined as a military [or corporate] adversary who tries to undermine his target's ability to wage war [do business] by attacking the adversary's information or network infrastructure (p. 56). Because of the importance of protecting confidential information, the U.S. government has been the principal bellwether in developing standards organizations as well as funding and developing information security guidelines and standards (Harris, 2003, p. 23).

Part Two: Overview of Threats and Vulnerabilities to an Information System

Part two of the Review of Literature describes and summarizes the most common threats and vulnerabilities to organizational information and information systems as well as explores their potential impact on organizational and business continuity (Krutz & Vines, 2001). This part also identifies barriers (Caralli et al., 2007) that impede the evolution of information security within organization.

Ross et al. (2007) state that information systems are incredibly complex assemblages of technology, processes, and people that collaboratively function together to accommodate the processing, storage, and transmission of information to support an organization's mission and business functions (Ross, et al., 2007, p. 1). The complexity of information systems creates challenges faced in securing information and the information systems. In order to provide contextual understanding of the meaning of threats, according to Harris (2003), it is important to make the distinction and understand the meanings of threat, vulnerability, and the assessment of risk.

Threats in the context of information security. A threat, according to Julia (2002), in the context of information security, is defined as anything that may compromise an asset (p. 13). Assets, in the context of information security, according the Julia (2002) are principally information, information systems hardware and software, and people; critical assets are those that are essential to meeting an organization's mission and business objectives (p. 13). For illustrative purposes, Table 1 provides a list of a few information assets common in business and government organizations (Scheier, 2003, p. 63).

COMMON INFORMATION ASSETS

Business	**Government**
Customer Databases	Military Strategy Data
Product Development Data	Weapons capabilities Data
Financial Data	Military Supply Chain Information
Employee Data	National Security & Intelligence

Marketing & Product Data	Internal Revenue Data
Strategic Planning Data	Import Export Data
Operational procedures	Judicial System Records
Trade Secrets	Emergency Preparedness Data

Table 1. Examples of Common Information Assets

According to Caralli (2004), regardless of what organizational assets are to be secured (information or technical assets, physical plant, or personnel), the organization must have a security strategy that can be implemented, measured, and revised as the business climate and operational environment change. He stresses that the effectiveness of a security strategy depends on how well it protects assets, which are critical to survivability and success of an organization, from identified threats (Caralli, p. 2).

The National Institute of Standards and Technology (NIST) uses the following definition of a threat in the context of information security as:

> "…any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability" (Kissel, 2006, p. 78).

Harris (2003) also iterates that a threat is something that, or someone who, will identify a specific vulnerability and use it against the organization or individual p. 56). He continues to explain that the entity that takes advantage of a vulnerability is referred to as a threat agent and risk is the likelihood of a threat agent taking advantage of a vulnerability.

Vulnerabilities within the context of information security. Harris (2003) describes vulnerability, as it relates to information security, as a software, hardware, or procedural weakness that may provide an attacker [threat agent] the open door the entity is looking for to enter a computer or network [information system] and have unauthorized access to resources within the environment. She emphasizes that vulnerability characterizes the absence or weakness of protection or safeguards (p. 56). In order to promote better understanding of the relationships among the different security components, Harris (2003) provides the following illustration, shown in *Figure 2*.

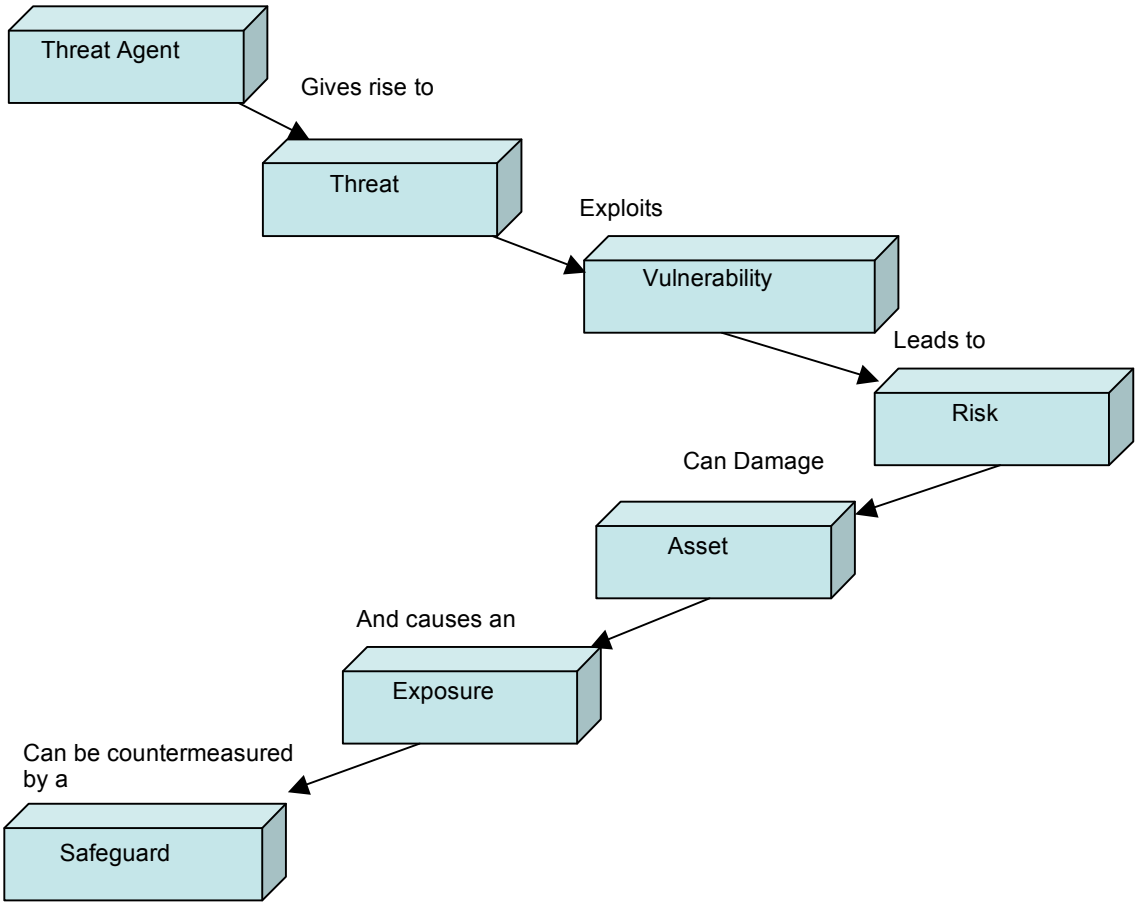

Figure 2 – Threat/Vulnerability Flow Chart (Harris, 2003, p. 57)

The Federal Financial Institutions Examination Council Information Security Exam Handbook, FFIEC (2006), defines vulnerabilities as weaknesses in a system or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. The FFIEC states that:

> "…vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing or other reviews of the environment, knowledge of policy weaknesses, knowledge of inadequate implementations, and knowledge of personnel issues. Adequate and timely testing is essential to identify many of these vulnerabilities. Expected vulnerabilities to consider are those that can reasonably be anticipated to arise in the future. Examples may include unpatched software, new and unique attack methodologies that bypass current controls, employee and contractor failures to perform security duties satisfactorily, personnel turnover resulting in less experienced and knowledgeable staff, new technology introduced with security flaws, and failure to comply with policies and procedures" (FFIEC, 2006, p. 1).

Threat agents. The *Federal Financial Institutions Examinations Council Information Security Handbook* FFIEC (2006) states that threats can be characterized as the potential for [threat] agents exploiting a vulnerability to cause harm through the unauthorized disclosure, misuse, alteration, or destruction of information or information systems. The FFIEC (2006) iterates that threats can arise from a wide variety of sources.

Threat agents have been categorized as internal (malicious or incompetent employees, contractors, service providers, and former insiders) and external (criminals, recreational hackers, competitors, and terrorists). Each of the [threat] agents identified may have different capabilities and motivations, which may require the use of different risk mitigation and control techniques and the focus on different information elements or systems. Natural and man-made disasters should also be considered as threat agents (FFIEC, 2006, p. 12). Bowen, Hash, & Wilson (2006) state threat identification consists of identifying threat sources with the potential to exploit weaknesses or vulnerabilities in an information system. They state that common threats to information and information systems can be categorized into three areas:

(1) Natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, electrical storms)

(2) Human threats (intentional or unintentional)

(3) Environmental threats (e.g., power failure) (p. 87).

Natural threats, such as floods earthquakes, tornadoes, landslides, avalanches, and electrical storms, are defined by Harris (2003) as physical threats to information security; these types of threats directly affect the facility or physical site hosting the information systems (p. 258). Scheier (2003) considers organizational adversaries (*human threats*) to be the greatest threat to information security. He states that adversaries in the digital world are the same as they are in the physical world and include: common criminals looking for financial gain, industrial spies looking for a competitive advantage, hackers, looking for secret knowledge, military-intelligence agencies looking for military intelligence (p. 42). Disgruntled current and former employees can present a substantial

threat to information and information systems (ISO-27002, 2005, p. 23). According to Krutz & Vines (2001), *environmental threats* affect the information system's operating environment. The following are the three main areas of environmental threats and controls as defined by Krutz & Vines (2001):

1. Electrical power
2. Fire detection and suppression
3. Heating, ventilation, and air conditioning (HVAC)

Krutz & Vines (2001) emphasize that information systems equipment including computers, servers, as well as networking and telecommunications equipment are sensitive and need a consistent level of humidity, temperature, and electrical power to function properly. Further, environmental threats can be caused by poor planning of the facility which hosts the operating environment of the information system (p. 332).

Risk assessment. The FFIEC (2006) states each organization should ultimately determine exactly what kinds of threats or vulnerabilities are most important to address in each particular organization's context through a process called risk assessment. The FFIEC defines risk assessment as the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. In its simplest form, a risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks (p. 9).

Organizational barriers to implementing information security strategy. Caralli (2004) stresses that the common barrier to implementing information security in many organizations is that organizations are ill-equipped to define their security goals and make explicit connections between their security goals and the strategic drivers and goals of the organization. Securing sponsorship of executive-level management is critical to securing resources for implementing information security in an organization (p. 6). Pettey (2005) argues that in order to overcome the challenges of developing information security strategy, organizations need an executive-level manager that understands information security technologies as well as business acumen. She states that this role is commonly known as the Chief Information Security Officer (CISO) and that this role is critical in communicating information security goals, needs, and strategy to upper management (n.d.). Harris (2006) emphasizes the importance of upper management involvement in the development of information security strategy and states that information security programs should always use a top-down approach, meaning that the initiation, support and direction come from upper management and work their way through middle management, and then to staff members in contrast with a bottom-up approach referring to situations in which the IT department tries to develop a security program without getting proper management support and direction (n.d.). Ultimately, information security strategy and goals should become an enabler of the organization's mission or strategy, rather than a burden or expense (Caralli, 2004, p. 6).

Part 3: Critical Elements of an Information Security Strategy

Using supporting arguments derived from the selected literature, part three of the Review of Literature identifies and presents ten critical elements of an information security strategy, as defined by the International Standards Organization (ISO-27002, 2005). It should be noted that the specific elements which ensure business continuity, minimizing business risk, and maximizing return on investments and business opportunities (ISO-27002, 2005, p. viii) may vary among organizations. As such, the International Standards Organization ISO-27002 *Security Techniques: Code of Practice for Information Security Management* handbook provides general guidelines and general principles for initiating, implementing, maintaining, and improving information security in public and private organization (ISO-27002, 2005, p. 1). The ten elements covered in this document are listed in Table 2. A discussion of each element follows.

1 Security Policy

2 Organizing Information Security

3 Asset Management

4 Human Resources Security

5 Physical and Environmental Security

6 Communications and Operations Management

7 Access Control

8 Information Systems Acquisition, Development and Maintenance

9 Business Continuity Management

10 Compliance with Legal Requirements

Table 2 (ISO-27002, 2005, p. 1)

#1 - Security Policy. ISO-27002 states that the objective of an information security policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization (ISO-27002, 2005, p. 7).

Information security policies according to Harris (2003) are high-level and are not necessarily technical in nature. They are drafted and put to use in order to protect the organization's assets by ensuring that mechanisms are established to protect organizational assets' confidentiality, availability, and integrity. She states that having an information security policy in place can also reduce legal liability by following the concept of due care and due diligence (Harris, 2003, p. 793).

Whitman & Mattord (2004) define policy as a set of rules that dictate acceptable and unacceptable behavior within an organization. They must also specify the penalties for unacceptable behavior and define an appeal process. A standard is a more detailed statement of what must be done to comply with policy. Practices, procedures, and guidelines explain how employees are expected to comply with policy *(Whitman & Mattord, 2004, p. 109).*

#2 - Organizing Information Security. This element is defined by ISO-27002 (2005) as the establishment of a management framework for information security within

the organization. The role of organizational management with regards to information security according to ISO-27002 is to:

- ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;
- formulate, review, and approve information security policy;
- review the effectiveness of the implementation of the information security policy;
- provide clear direction and visible management support for security initiatives;
- provide the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across the organization;
- initiate plans and programs to maintain information security awareness;
- ensure that the implementation of information security controls is co-ordinated across the organization (ISO-27002, 2005, p. 9).

ISO-27002 (2005) states that management should actively promote and support information security within the organization through: clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities (p. 9). ISO-27002 recommends that all information security responsibilities should be clearly defined in the following ways:

- Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

- A management authorization process for new information processing facilities should be defined and implemented.
- Appropriate contacts with relevant authorities should be maintained.
- Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.
- The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
- Identification of risks related to external parties Control The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

#3 - Asset Management. ISO-27002 states that an organization needs to know what assets need to be secured and therefore an information security strategy should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value (ISO-27002, 2005, p. 19).

Whitman & Mattord (2004) state that proper information security via risk identification begins with the classification and identification of assets where each information asset is identified, categorized, classified, and a value is assigned. They state

that this process is important in order assure that the most valuable information assets are given the highest priority and are secured (p. 295).

The implementation of specific information security controls may be delegated by the owner or responsible party as appropriate but the owner still remains responsible for the proper protection of the assets (ISO-27002, 2005, p. 19). ISO-27002 also emphasizes that owners or responsible parties should be identified for all assets and that they be given the responsibility for the maintenance of appropriate information security control.

#4 - Human Resources Security. ISO-27002 states the securing human resources should ensure that employees, contractors and third party users understand their responsibilities and are suitable for the roles they are performing. The goal is to reduce the risk of theft, fraud or misuse of facilities. ISO states that security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment and that all candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs. ISO further iterates that employees, contractors and third party users of information processing facilities should understand the terms and conditions of employment and always sign an agreement or contract as to their security roles and responsibilities (ISO-27002, 2005, p. 23).

Security screening and background checks, according to Whitman & Mattord (2004), can uncover past criminal behavior or other information that suggest a potential for future misconduct or a vulnerability that might render a candidate susceptible to coercion or blackmail. Whitman and Mattord (2004) state that when employees leave an organization there are several security issues to be considered (p. 438). ISO-27002 adds

that responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.

ISO-27002 emphasizes that information security awareness, education, and training is an essential component of human resource security which should ensure that an organization's employees and, where relevant, contractors and third party users should receive an appropriate level of information security awareness training and regular updates in organizational policies and procedures, as relevant for their job function (ISO-27002, 2005, p. 26). Pironti (2006) states that in order for information security awareness, education, and training to be effective, it must be flexible enough to allow personalization and localization to the audience with which it is attempting to educate and should address language, culture, as well as role considerations within the organization (p. 4). Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role (ISO-27002, 2005, p. 26).

Information security awareness and training, according to Wilson & Hash (2003) should be focused on the organization's entire user population. They advise that an information security awareness program should be aimed at all levels of the organization including senior and executive managers and that the effectiveness of this effort will usually determine the effectiveness of the awareness and training program (Wilson & Hash, 2003, p. 7).

Wilson & Hash (2003) emphasize that users are the largest audience in any organization and are the single most important group of people who can help to reduce

unintentional errors and IT vulnerabilities. They point out that users may include employees, contractors, visitors, guests, and other collaborators or associates requiring access (Wilson & Hash, 2003, p. 5). They state that information security awareness and training should at a minimum enable users to:

1. Understand and comply with agency security policies and procedures;
2. Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
3. Work with management to meet training needs;
4. Keep software applications updated with security patches;
5. Be aware of actions they can take to better protect their agency's information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms (Wilson & Hash, 2003, p. 5).

#5 - Physical and Environmental Security. The objective of Physical and Environmental Security, following the guidelines of ISO-27002, is to prevent unauthorized physical access, damage, and interference to the and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate physical security barriers and physical entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified

risks and are intended to mitigate natural and environment threats (ISO-27002, 2005, p. 29).

The Physical and Environmental Security element of an information security strategy, according to Harris (2003) should address physical site design and layout, environmental components, emergency response readiness, training, physical access control, intrusion detection, electrical power and fire protection. She summarizes by stating that Physical and Environmental Security mechanisms protect people, data, equipment, systems, and the facility itself (Harris, 2003, p. 253).

#6 - Communications and Operations Management. According to Harris (2003), the Communications and Operations Management element of information security strategy pertains to everything that takes place to keep a network, computer systems, applications, and environment up and running in secure and protected manner. She states that communication networks and computing environments are "evolving entities and require continual and day-to-day maintenance (p. 753).

ISO-27002 states that in order to provide consistency and predictability of information security operations, operating procedures should be documented, maintained, and made available to all users who need them. ISO-27002 recommends that documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety (ISO-27002, 2005, p. 37)

Another part of Security Operations management is third party service delivery management. ISO-27002 suggests that organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party (ISO-27002, 2005, p. 37)

Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use (ISO-27002, 2005, p. 37). Harris (2003) states that products should always be evaluated for the level of trust and assurance they provide and that there be an agreed upon and documented procedure for evaluating products and components of a data communications network and information system (Harris, 2003, p. 757).

Software and information processing facilities, following ISO-27002, are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. ISO recommends that all users of information systems should be made aware of the dangers and ramifications of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code (ISO-27002, 2005, p. 42).

An essential part of the ongoing management of information security operations is ensuring that information is backed up and can be restored reliably (Harris, 2003, p. 559). ISO-27002 recommends that a backup policy should be developed and that back-up copies of information and software should be taken and regularly tested in accordance with such a policy. ISO-27002 emphasizes that adequate back-up facilities should be

provided to ensure that all essential information and software can be recovered following a disaster or media failure and that appropriate operating procedures should be established to protect documents, computer media (e.g.tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction. (ISO-27002, 2005, p. 42).

Electronic mail (Email) communication is a critical and integral component of organization's today and yet it is an insecure communications media in that it can be easily intercepted and fraudulently modified (Harris, 2003, p. 763). ISO-27002 suggests that information exchange, such as email, should use encryption wherever possible and that all network systems that support the relaying of email and information be monitored and configured with appropriate levels of access control (ISO-27002, 2005, p. 42).

#7 - Access Control. Proper access control, as stated by Harris (2003), should be included in an information security strategy to control a user's as well as software's ability to view or modify information and access or communicate with a component of an information system. Access control policy and mechanisms should ultimately manage the flow of information between users and information systems as well as intercommunication between disparate information systems (Harris, 2003, p. 867).

ISO-27002 (2005) points out elements of access control which need to be addressed in an information security strategy through policies, standards, and documented procedures in *Table 3*:

Access Control Policy

User access management

Network Access Control

Operating System Access Control

Software Application access Control

Information Access Restriction (i.e.,database, file and folder access control)

Mobile Computing, Remote Access, and Teleworking

Table 3 (ISO-27002, 2005, pp. 60-76)

For further reference, the ISO-27002 standards document (see pages 60 through 76) provides an excellent and exhaustive explanation and implementation plan these identified elements of access control.

#8 - Information Systems Acquisition, Development and Maintenance.

Information security policy and controls should be put in place that address the acquisition, development, and maintenance of information systems. According to ISO-27002, because organizations depend on operating systems, infrastructure, business applications, off-the-shelf software, services, as well as in-house developed applications, there must be a defined policy governing and controlling the planning, procurement, and implementation of such information technology. ISO-27002 also state that "security requirements must be identified at the requirements phase of a project and should be justified, agreed, and documented as part of the overall business case for an information systems (ISO-27002, 2003, p. 77).

#9 - Business Continuity Management. Honour (n.d.) states that Business Continuity Management (BCP) is a complex and quickly evolving element of

information security management and is difficult to define. He states that Business Continuity Management can be defined as a "holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities" (Honour, n.d.). He adds that Business continuity is also "the management of recovery or continuity in the event of a disaster" as well as the "management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date" (Honour, n.d.).

ISO-27002 (2005) articulates that the overall objective of the information security aspects of business continuity management is to counteract interruptions to business [organizational] activities and to protect critical business process from the catastrophic effects of "major failures" of information systems or disasters [natural and man-made]. The goal is to "ensure their timely resumption" and should provide controls to continuously identify and reduce risks, confine the consequences of damaging incidents, and ensure that information required for business processes is readily available (p. 95). The consequences of exploited threats such as disasters, security, failures, loss of service, and service availability, according to ISO-27002 (2005), should be addressed in a business continuity plan that includes information security as an integral of the entire business continuity process.

Harris (2003) concurs and affirms that main goal of business continuity is to resume organizational functionality and business as quickly as possible and that the overall plan should cover all organizational elements, identify critical service and functions, provide alternatives for emergency operations, and integrate each autonomous departmental plan

(p. 563). *Figure 3* illustrates how each department must have their own BCP plan under the overall enterprise-wide plan:

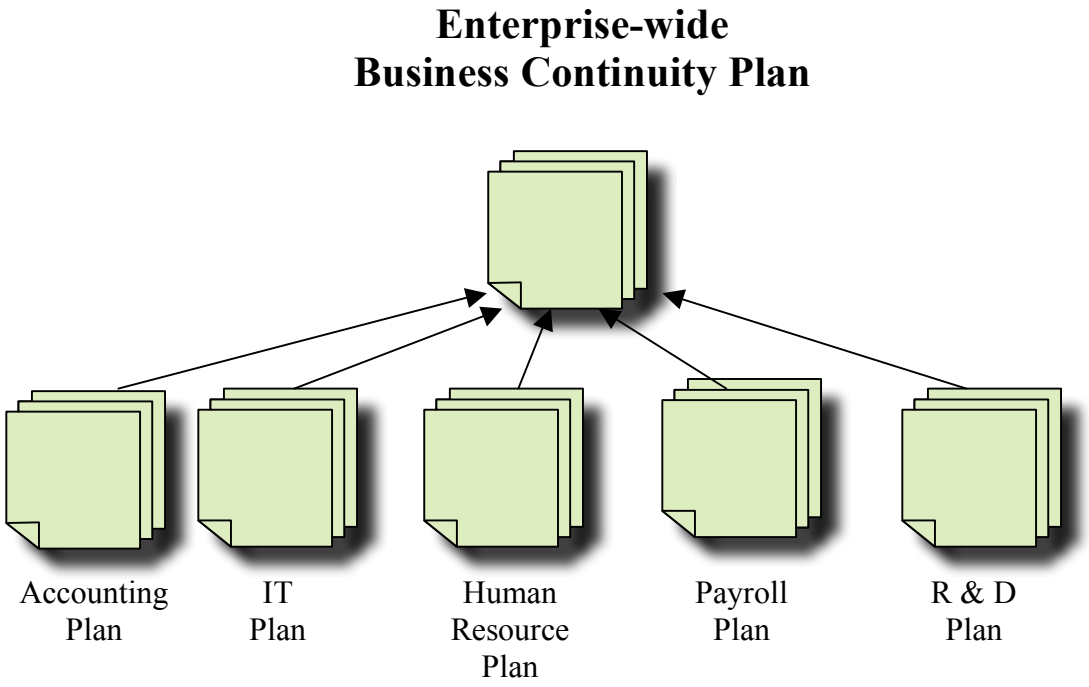

Figure 3. Business Continuity Plan Integration Example (Harris, 2003, p. 564)

Harris (2003) states that an organization should have a dedicated "team" of staff which is responsible for the overall development, implementation and maintenance of the organization's business continuity plan. She emphasizes that both established management and the business continuity planning team both have distinct and equally important responsibilities. Tables 4 and 5 below provide a list of these common BCP responsibilities.:

Management Responsibilities
Full Commitment to the BCP initiative
Policy and goal setting
Making available the necessary funds and resources
Taking responsibility for the outcome of the development of the BCP
Appointing a BCP team

Table 4. (Harris, 2003, p. 564)

BCP Team Responsibilities
Identifying regulatory and legal requirements that must be met
Identifying all possible threats and risks
Estimating the possibilities of the threats and the loss potential and impact to the organization
Outlining which departments, systems, and processes must be up and running before any others
Developing procedures and steps in resuming business after a disaster

Table 5. (Harris, 2003, p. 564)

#10 - Compliance with Legal Requirements. Whitman & Mattord (2004) state that information security professionals must possess at least a rudimentary grasp of the "legal framework" in which their organizations operate (p. 453). The purpose of this element of information security strategy, according to ISO-27002 (2005) is to ensure compliance to legal requirements "in order to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements" (ISO-27002, 2005, p. 100).

Harris (2003) also points out that the computer and information crimes are the result of society's growing dependence upon information technology. She adds that, for example, fraud, theft, and embezzlement have always occurred and that as e-commerce and online business continue to become a part of today's business world, these types of crimes become more dangerous (p. 595).

ISO-27002 (2005) states that the design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements and that advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. ISO-27002 adds that legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow) (ISO-27002, 2005, p. 100).

Conclusion

The overall purpose of this literature review has been to address the issues that organizations must define in order to develop an effective information security strategy (FFIEC, 2006, p. 21.). The Conclusion provides discussion of specific elements that should be considered. Additional focus for the needs of the audience is presented through the use of eight tables and one figure, adapted from selected references (Sevilla, 2002, p. 145).

Pironti (2006) states that the establishment of an information security strategy is cornerstone in transforming information security into a more effective proactive activity driven by organizational leadership, in contrast to the typical reactive model of information security driven by technologists (p. 1). Harris (2006) adds that every organization's approach to a security strategy should be different and customized accordingly, because each organization has its own threats, risks, business drivers, and industry compliance requirements (n.d.)..

Understanding the historical and cultural context of information security in private and public organizations provides the information security professional an important piece of the foundational knowledge in understanding the importance of an information strategy. This literature review reveals the common threats, vulnerabilities, and the controls that can be used to mitigate said threats and vulnerabilities. When designing an information security management strategy, professionals should begin with development and adoption of a formal approach to addressing organizational information security Figure 4 illustrates how policies are the foundation on which organizational

standards, practices, guidelines, and procedures are developed, according to Whitman & Mattord (2004).

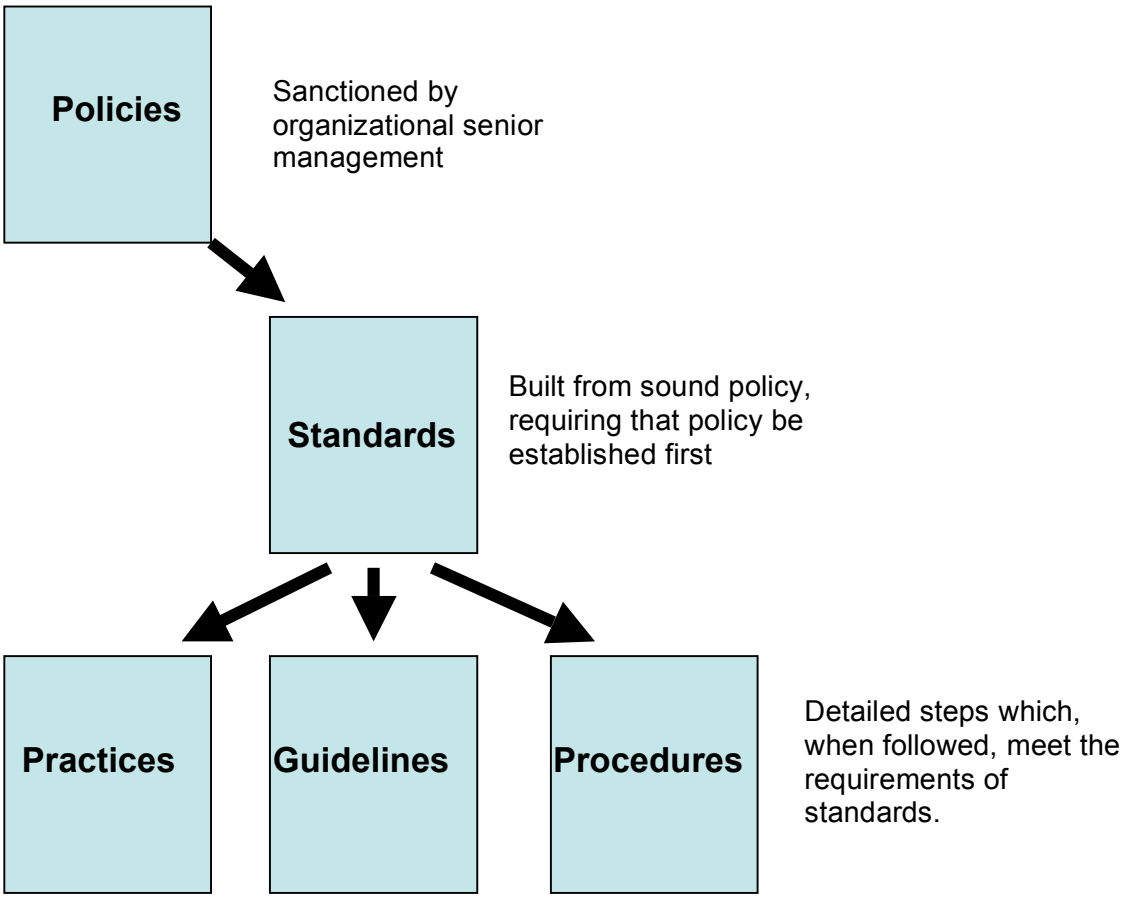

Figure 4. Hierarchy of Policy, Standards, Practices, Guidelines, & Procedures (Whitman & Mattord, 2004, p. 109)

Additionally, the literature review provides a baseline overview of the elements and sub-elements which are recommended by the International Standards Organization ISO-27002 handbook *Security Techniques: Code of practice for Information Security Management,* supported by the perspectives of selected authors in the field of information security. According to ISO-27002 (2005), an information security policy document should contain six key components, provided in Table 6.

Six Key Information Security Policy Components	
1	A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
2	A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives
3	A framework for setting control objectives and controls, including the structure of risk assessment and risk management
4	A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including: compliance with legislative, regulatory, and contractual requirements security education
5	A definition of general and specific responsibilities for information security management, including reporting information security incidents
6	References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules with which users should comply

Table 6. Six Key Policy Components (ISO-27002, 2005, p. 5)

ISO-27002 recommends that in order to ensure that information is properly implemented and managed, all information security responsibilities must be clearly defined. Table 7 provides a brief list of responsibilities and approaches to be defined within an organization.

Information Security Responsibilities

1	Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions
2	A management authorization process for new information processing facilities should be defined and implemented
3	Appropriate contacts with relevant authorities should be maintained
4	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained
5	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur
6	Identification of risks related to external parties. The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access

Table 7. Information Security Responsibilities, (ISO-27002, 2005, p. 9)

ISO-27002 states that there are many types of assets that organizations must identify and protect. Table 8 illustrates the most common examples.

Examples of Common Assets	**Description**
Information	Databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information

Software	Application software, system software, development tools, and utilities
Physical	Computer equipment, communications equipment, removable media, and other equipment
Service	Computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning
People	Their qualifications, skills, and experience
Intangibles	Such as reputation and image of the organization

Table 8. Examples of Common Assets, (ISO-27002, 2005, p. 19)

Whitman & Mattord (2004) state that current and former employees can potentially present the greatest threats to information security. As such, Human Resource elements of an information security strategy need to be addressed (p. 438). To help address security concerns in hiring employees, Whitman & Mattord (2004) provide a list of recommended background checks to be performed in the hiring process, presented in Table 9.

Human Resource Security: Background Check Recommendations

Identity checks

Education and credential checks: institutions attended, degrees and

certifications earned, and certification status

Previous employment verification

Reference checks: validity of references and integrity of reference sources

Worker's compensation history including worker's comp claims

DMV records

Drug history: drug screening and history of drug arrests

Medical History

Credit history: credit problems, financial problems, and bankruptcy

Criminal and Civil court history

Table 9. Necessary Background Checks, (Whitman & Mattord, 2004, p. 438)

An information security awareness and training program contributes to improved security in an organization. Wilson & Hash (2003) illustrate five key ways in which an information security awareness and training helps employees, as synthesized in Table 10.

	Information Security Awareness Training enables users to:
1	Understand and comply with agency security policies and procedures
2	

	Be appropriately trained in the rules of behavior for the systems and applications to which they have access
3	Work with management to meet training needs
4	Keep software applications updated with security patches
5	Be aware of actions they can take to better protect their agency's information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms

Table 10. Information Awareness Training, (Wilson & Hash, 2003, p. 5).

When employees leave an organization Whitman & Mattord (2004) recommend that Human Resources should employ an exiting security procedure. Elements are outlined in Table 11.

	Employee Exiting Security Procedure
1	Disable access to all organizational systems
2	Retrieve all removable media
3	Secure hard drives
4	Change file cabinet locks

5	Change office door locks
6	Revoke former keycard access
7	Remove personal effects from premises
8	Personally escort former employer office once keys, keycards, and other business property have been turned over.

Table 11. Employee Exiting Procedure, (Whitman & Mattord, 2004, p. 438)

ISO-27002 emphasizes that assessing physical and environment risk and threats requires working in conjunction with facilities personnel. Such work can provide information security teams insight into how to properly address threats to information processing facilities. This work also has potential to provide a baseline from which controls can be developed to mitigate such threats (ISO-27002, 2005, p. 29).

According to ISO-27002, in order to provide for secure operation of information processing facilities, an information security strategy should address Communication and Operations Management. The ISO-27002 standard states that "responsibilities and procedures for the management and operation of all information processing facilities should be established (ISO-27002, 2005, p. 37). Policies and procedures should be put in place and followed closely in regards to the acquisition, development, procurement, and maintenance of the components of information systems. Table 12 provides a set of

security controls and their descriptions for Information Systems Acquisition, Development and Maintenance.

System Control	Description
Information Systems Requirements	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls
Correct Processing in Applications	Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data
Cryptographic Controls	To protect the confidentiality, authenticity or integrity of information by cryptographic means a policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.
Security of System Files	To ensure the security of system files access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.
Development and Support Processes	To maintain the security of application system software and information project and support environments should be strictly controlled. Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

Technical Vulnerability Management	To reduce risks resulting from exploitation of published technical vulnerabilities technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

Table 12. System Controls, (ISO-27002, 2003, pp. 77-89)

Business Continuity Management, according to Harris (2003) is a critical element of information security which requires that upper management play a central role. She states that management must understand the consequence of risks and potential loss value, and cautions against merely paying "lip service," which, she states is worse than not having continuity plans at all due to the "false sense of security"(Harris, 2003, p. 558). Table 13 provides a list of important elements of business continuity management to be considered in an information security strategy.

Business Continuity Management Element	**Description**
Including Information Security in the Business Continuity Management Process	A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
Business Continuity and Risk Assessment	Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security

Developing and Implementing Continuity plans Emphasizing Information Security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes
Business Continuity Planning Framework	A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance
Testing, Maintaining and Re-assessing Business Continuity Plans	Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective

Table 13. Business Continuity Management Elements, (ISO-27002, 2005, p. 95)

Because information and information systems are subject to statutory, regulatory, and contractual security requirements (ISO-27002, 2005), due diligence requires that such legal requirements be addressed in an information strategy. ISO-27002 provides some general areas to be covered in a legal compliance initiatives (see Table 14 below).

Areas of Legal Compliance	Description
Develop legal records for all areas	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization
Intellectual property rights (IPR)	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of

	proprietary software products
Identification of applicable legislation	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization
Intellectual property rights (IPR)	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products
Protection of organizational records	Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements
Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses

Table 14. Legal Compliance Areas, (ISO-27002, 2005, pp. 100 – 106)

References

Allen, J. (2002) The CERT ® Guide to System and Network Security Practices. Upper Saddle River, NJ: Addison-Wesley

Bell, C., & Smith, C. (2008). *Critical Evaluation of Information Sources*. Retrieved April 27, 2008 from University of Oregon Web site: http://libweb.uoregon.edu/guides/findarticles/credibility.html

Bowen, P., Hash, J.,& Wilson, M.(2006) Information Security Handbook: *A Guide for Managers. National Institute of Standards and Technology publication 800-100*. Retrieved April 14, 2008 from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Canal, V.A.(2005, Sept) *On Information Security Paradigms*. Information Systems Security Association (ISSA(R)) Journal [Online Version]. Retrieved May, 19, 2008 from https://www.issa.org/Library/Journals/2005/September/Aceituno%20Canal%20-%20On%20Information%20Security%20Paradigms.pdf

Caralli, R. (2004) The Critical Success Factor Method: *Establishing a Foundation for Enterprise Security Management. Carnegie-Mellon Engineering Institute Journal Article*. Retrieved April 9, 2008 from

http://www.cert.org/archive/pdf/criticalsuccessfactors0407.pdf

Caralli, R., Stevens, C., Wallen, D., White, W., Wilson,W., & Young, L. (2007) Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes. Technical Report CMU/SEI-2007-TR-009 ESC-TR-2007-009 Carnegie - Mellon University. Retrieved May 5, 2008 from www.cert.org/archive/pdf/07tr009.pdf

CISO (n.d) *Web Site for Chief Information Security Officer Description*. Retrieved April 17, 2007 from http://www.chiefinformationsecurityofficer.com/

Colorado State University (n.d.) *What is a Review Paper*. Writing Guide from the Colorado State University Writing Center. Retrieved April 24, 2008 from http://writing.colostate.edu/guides/documents/review_essay/pop2a.cfm

CNSS (2007) *Committee on National Security Systems - National Information Assurance Glossary*. [E-Version] Retrieved April 14, 2008 from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

CSO-Undercover (2007) *How Establishing a Security Management Team Allows Leaders to Focus on Strategy*. Retrieved April 17, 2008 from http://www.cio.com/article/139100/How_Establishing_a_Security_Management_Team_Allows_Leaders_to_Focus_on_Strategy

E-Literal (n.d.) *Decisions Support System Glossary*. Retrieved April 16, 2008 from http://services.eliteral.com/glossary/decision-support-systems-glossary.php

FFIEC (2006) *IT Handbook InfoBase*. Retrieved April 17, 2008 from http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

Harris, S. (2003) *Certified Information Systems Security Professional (CISSP) All-In-One Exam Guide 2nd ed*. Emeryville, CA: McGraw-Hill / Osborne.

Harris, S. (2006) *Risk Management: Key elements when building an information security Program*. Article Retrieved May 7, 2008 from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210562,00.html

Hewitt, M. (1998) Trent Focus for Research and Development in Primary Health Care: *Carrying Out a Literature Review*. Retrieved April 8, 2008 from http://128.223.179.107/aim/Capstone07/HewittLitReview.pdf

HIPAA(n,d) *Medical Dictionary Definition* Retrieved May 20, 2008 from http://www.medterms.com/script/main/art.asp?articlekey=31785

Honour, D. (Ed.) (n.d.) *Defining Business Continuity*. Web Article. Retrieved April 17, 2008 from http://www.continuitycentral.com/feature0398.htm

International Standards Organization (n.d) Retrieved May 27, 2008 from http://www.iso.org/iso/about.htm

ISO-27002 (2005) Information technology Security techniques: *Code of practice for Information Security management*. International Standards Organization (ISO) document. Reference number ISO/IEC 27002:2005(E).

(ISC)² (2008, n.d) *The International Information Systems Security Certification Consortium, Inc.* [Website] https://www.isc2.org/cgi-bin/content.cgi?category=84

Jenkins, G. (1999) Information Systems: *Policies and Procedures Manual.* Paramus, NJ: Prentice Hall

Kissel, R. (Ed.) (2006) National Institute of Standards and Technology: *Glossary of Key Information Security Terms*. [E-Version] Retrieved April 15, 2008 from http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

Krutz, R. & Vines, R. (2001) CISSP Prep Guide: *Mastering the Ten Domains of Information Security*. New York, N.Y.: Wiley & Sons.

Leedy, P. & Ormrod, J (2005) Practical Research: *Planning and Design* (8th ed.). Saddle River, NJ: Pearson Merrill Prentice Hall.

Lewis University (n.d.) *A Brief History of Information Security*. Online article Retrieved

May 29, 2008 from http://www.lewisu.edu/academics/msinfosec/history.htm

Lucas, A. (n.d) Thomas Jefferson Wheel Cypher. Online Article Retrieved May 25, 2008 from http://www.monticello.org/reports/interests/wheel_cipher.html

Nahra, K.& Rein, W. (2007, February) Experience *Highlights Need For Data Security Vigilance*. Metropolitan Corporate Counsel Journal. Retrieved May 4, 2008 from http://www.metrocorpcounsel.com/current.php?artType=view&EntryNo=6280

Obenzinger, H. (2005) *"What Can a Literature Review Do For Me?;" How to Research, Write, and Survive a Literature Review.* Retrieved April15, 2007, from http://128.223.179.107/aim/Capstone07/LiteratureReviewHandout.pdf

Ormondroyd, J., Engle, M., & Cosgrave, T. (2004). *Critically Analyzing Information Sources*. Retrieved April 27, 2007, from Cornell University Library Web site: http://www.library.cornell.edu/olinuris/ref/research/skill26.htm#

Peltier, T. (2005) *Information Risk Analysis*. Boca Raton, FL: Auerbach Publications

Pettey, C.(2005) Gartner *Highlights the Evolving Role of CISO in the New Security Order.* Online Article Retrieved May 16, 2008 from http://www.gartner.com/press_releases/asset_135714_11.html

Pironti, J. (2005) *Key Elements of an Information Security Program*. Information

Systems Control Journal, Vol. 1. Retrieved April 14, 2008 from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23540

Ross, R. Johnson, A., Katzke, S., Toth, P., Stoneburner, G., Rogers, G, (2007) *Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans. NIST Special Publication 800-53A*. Retrieved April 14, 2007 from http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf

Schneier, B. (2004) Secrets & Lies: *Digital Security in a Networked World*. Indianapolis, Ind.: Wiley Publishing Inc.

Sevilla, C. (2002) *Information Design Desk Reference*. Menlo Park, CA.: Crisp Publications.

Sundaram, A. (2008, May) Security Metrics: *Hype, reality, and value demonstration.* Information Systems Security Association (ISSA$^{(R)}$) Journal 24 – 29.

TIR (2008) *Responsibility and Job Description of the Information Security Manager*. The Informatics Review website is an E-Journal of the Association of Medical Directors of Information Systems. Retrieved April 27, 2008 from http://www.informatics-review.com/jobdesc/infsec.html

University of North Carolina (n.d.) *Literature Reviews Handout* from University of North Carolina.. Retrieved April 23, 2008 from www.unc.edu/depts/wcweb/handouts/literature_review.html

Von Solms, E. & Von Solms, S.H. (2000) *Information Security Management Through Measurement*. In S. Qing & J.H.P. Eloff (Eds.) *Information Security for Global Information Infrastructures* (pp. 59 – 68). Norwell, MA: Kurwell Academic

Warren. M. & Hutchinson, W (2000) *Information Warfare: Fact or Fiction* In S. Qing & J.H.P. Eloff (Eds.) *Information Security for Global Information Infrastructures* (pp. 411 - 420). Norwell, MA: Kurwell Academic

Whitman, M., & Mattord., (2004) *Management of Information Security*. Boston, Ma: Thomson.

Wilson. M & Hash, J. (2003) *Building an Information Technology Security Awareness and Training Program*. National Institute of Standards Technology (NIST) Special Publication 800-50. Retrieved May 5, 2008 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Yourdin, E. (2002) Byte Wars: *The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall.

ZDNET (n,d) Ziff Davis Publishers (ZDNET) *Definition for Compliance*. Retrieved May 20, 2008 from http://dictionary.zdnet.com/definition/Compliance.html